TITLE: Data Protection Policy

Effective Date	25 May 2018	**Version**	03
Approved By	Management Board	**Date Approved**	23 May 2018
		Review Date	23 May 2021 or as required
Superseded or Obsolete Policy / Procedure(s)		**Owner**	
02 - Data Protection Policy		Data Protection Officer	

Contents

1. Purpose of Policy

The General Data Protection Regulation (EU) 2016/679 (hereafter GDPR) governs the processing of personal data in the European Union (hereafter EU). Important objectives of the legislation are to safeguard the data protection rights of living individuals and to set out the obligations of persons who process personal data. The GDPR is transposed directly into national law. It permits national legislation in some areas, hence the continued applicability of the Irish Data Protection Acts (a new Act is forthcoming).

This Policy is a statement of Carlow College's commitment to uphold the data protection rights of persons with whom it comes into contact; acknowledges Carlow College's statutory responsibilities; and outlines Carlow College's procedures for responding to those responsibilities.

Carlow College falls within the remit of the Freedom of Information Act 2014, which also, inter alia, refers to personal information. This Policy is to be read in conjunction with the College's Freedom of Information Policy, Records Management Policy and any other policy, procedure or College document which alludes to Data Protection. Reference to the Data Protection Acts 1988 and 2003 in such documents is now to be taken to mean the GDPR and national legislation.

Carlow College requires to process personal data of various persons with whom it comes into contact, for instance, employees, learners and other stakeholders, including members of the public. Detailed information regarding the processing of personal data is set out in the College's Privacy Notices, which are available on our website.

2. Definitions

The following definitions are taken or adapted from the GDPR.

Personal data means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Data concerning criminal convictions was 'sensitive personal data' under the Data Protection Acts 1988 and 2003. It is not special category data under the GDPR but continues to benefit from special protection.

Processing means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. In short, any action between collection and destruction is likel y processing.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. Carlow College student numbers constitute personal data of registered learners. They cannot be used to pseudonymise references to learners.

Anonymous information is information which does not relate to an identified or identifiable natural person, or it is personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. The GPDR does not apply to the processing of anonymous information, including for statistical or research purposes.

Filing system means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Controller means the natural or legal person which alone or jointly with others, determines the purposes and means of the processing of personal data. Carlow College is a controller in some instances.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Carlow College is a processor in some instances.

Recipient means a natural or legal person, public authority, agency or other body, to which the personal data are disclosed, whether a third party or not. Public authorities which may receive personal data in the framework of a particular inquiry in accordance with EU or Member State law are not recipients.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. Scope of Policy

This Policy applies to any natural or legal person who is employed, contracted or otherwise engaged by Carlow College in any capacity, and who processes personal data on behalf of the College for administrative, management, academic, research or any other purpose.[1] Where the word 'employee' is used in this Policy and Associated Documentation it is intended to cover all situations where there is an employment

[1] Carlow College, St. Patrick's Students' Union does not come within the scope of this Policy.

relationship, regardless of whether the relationship is based on an employment contract, a volunteer agreement or a contract for services.

For example, this Policy applies, but is not limited to, employees, service providers, members of the Governing Body, external examiners, examinations invigilators and volunteers. This list is not exhaustive.

Any learner or employee of Carlow College who processes personal data in the course of research is expected to abide by data protection principles.

4. Policy Statement

Under the GDPR, individuals (data subjects) have various rights, and controllers and processors have a number of obligations and rights. These respective rights and obligations and Carlow College's procedures for responding to them are outlined in the following sections. The GDPR is risk-based legislation. Carlow College's procedures around data processing and safeguards take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

4.1 Data Protection Principles

A number of principles governing the processing of personal data are set out in the GDPR. Carlow College abides by these principles. They state shall that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not considered to be incompatible with the initial purposes (purpose limitation);
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (accuracy);
- Kept in a form which permits the identification of data subjects for no longer than is necessary. Personal data may be stored for longer periods in so far as it will be used solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of appropriate measures in order to safeguard the rights and freedoms of data subjects (storage limitation);
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures (integrity and confidentiality).

Carlow College uses a wide range of organisational and technical controls to ensure compliance with these principles, and that compliance is demonstrable in accordance with the accountability principle of the GDPR. Such measures include robust technical security protecting our IT systems, various access controls to personal data, data quality controls, the carrying out of Data Protection Impact Assessments, documented policies and procedures such as Records Retention Schedules, a Records Destruction Procedure, a Personal Data Breach Response Plan, provision of training to staff, employment of a Data Protection Officer (DPO) and contracts and agreements with processors and joint controllers respectively.

4.2 Lawfulness of processing personal data

The processing of personal data is lawful only if at least one of the bases outlined in Article 6 of the GDPR is relevant. Carlow College has identified a lawful basis for its processing of various personal data and this is documented in our Privacy Notices.

The following are the lawful bases set out in Article 6:

- The data subject has given consent to the processing for one or more specific purposes;
- Processing is necessary to the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the controller is subject. There must be a basis for such processing in EU or Member State law;
- Processing is necessary in order to protect the vital interests of the data subject or another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. There must a basis for such processing in EU or Member State law;
- Processing is necessary for the purposes of the legitimate interests pursued by the controller, or by a third party, except where such interests are overridden by the interests or fundamental rights of the data subject, which require protection of personal data, in particular where the data subject is a child.

Employees are to collect as little personal data as possible in order to achieve their purpose.

Many of the bases in Article 6 specify that processing must be ‘necessary’. Employees should ensure that the data processing is necessary for their purpose. If there is a less intrusive method of achieving the purpose, for example, the collection of less personal data, this method should be chosen.

4.3 Further processing

Personal data is collected for purposes which are specified in our Privacy Notices and Records of Processing Activities (available on the Staff Portal). Employees are to ensure compliance with these documents. Where an employee wishes to use personal

data for a new or different purpose than that listed he/she is to contact the DPO prior to beginning the processing.

Contact the DPO if you wish to use personal data for a new or different purpose.

.

The GDPR contains a list of factors to be taken into account to ascertain whether the further processing (which is not based on consent or an EU or Member State law) is compatible with the original purpose:

- Any link between the original purpose and the further processing purpose;
- The context in which the personal data was collected, in particular the relationship between the data subjects and the controller;
- The nature of the personal data, in particular, whether special category or criminal data is processed;
- The possible consequences of the further processing for data subjects;
- The existence of appropriate safeguards, including encryption or pseudonymisation.

A new lawful basis may not be needed if the new purpose is compatible with the original purpose. Further processing for archiving purposes in the public interest, for scientific and historical research purposes or for statistical purposes should be considered as compatible processing. If the original processing is based on consent, it will be necessary either to get fresh consent from the data subject which specifically covers the new processing or to find a different basis for the further processing.

4.4 Processing special categories of personal data

'Special categories of personal data' are a sub-category of 'personal data'. Due to the sensitive nature of such data it attracts extra safeguards. The bases upon which Carlow College processes such data are set out in the Privacy Notice and Records of Processing Activities. Employees must ensure compliance with these documents and contact the DPO in the event of uncertainty.

Take extra care with 'special categories of personal data'. Ensure compliance with the Privacy Notices and Records of Processing Activities. Contact the DPO in the event of uncertainty.

The processing of special categories of personal data is prohibited unless one of the legal bases set out in Article 9 of the GDPR applies. In addition, at least one of the legal bases outlined in Article 6 must apply.

The Article 9 bases include, inter alia:

- The data subject has given explicit consent to the processing;
- Processing is necessary for the obligations or rights of the controller or data subject in the field of employment and social security and social protection law in so far as it is authorised by EU or Member State law or a collective agreement pursuant to Member State law;
- Processing is necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent. This would be a life or death situation;

- Processing is carried out in the course of its legitimate interests by a foundation, association or not-for-profit body with a political, philosophical, religious or trade union aim;
- Processing relates to personal data manifestly made public by the data subject;
- Processing is necessary for the establishment, exercise or defence of legal claims;
- Processing is necessary for reasons of substantial public interest, on the basis of EU or Member State law;
- Processing is necessary for medical purposes, for the assessment of the working capacity of the employee, the provision of health or social care or treatment or the management of health or social care systems and services pursuant to EU or Member State law or pursuant to contract with a health professional and subject to conditions and safeguards;
- Processing is necessary for reasons of public interest in the area of public health eg epidemic;
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes in accordance with Article 89(1) based on Union or Member State law.

The GDPR considers that photographs are not automatically considered as special category personal data, for example, if a person's race may be determined from the photograph. Photographs are only considered as such if they allow the unique identification or authentication of an individual as a biometric (for example, in an electronic passport). However, photographs may be personal data and should be treated in the same way as other records.

4.5 Data relating to criminal convictions and offences

Such data was 'sensitive personal data' under the Data Protection Acts 1988 and 2003 but is not now covered under the analogous heading of 'special categories of personal data' in the GDPR.

However, such data continues to benefit from special protections under the GDPR.
As a 'relevant organisation' under the National Vetting Bureau (Children and Vulnerable Persons) Act 2012 to 2016, Carlow College must vet employees and learners whose activities bring them into contact with children and vulnerable persons. Records arising from the vetting process are managed in accordance with the College's Garda Vetting Policy.

4.6 Data processing on 'legitimate interest' grounds

Carlow College processes some personal data on legitimate interest grounds, as is permissible under Article 6 of the GDPR, and as detailed in the Privacy Notices. Examples of Carlow College's legitimate interests might be the security of its premises and IT systems, management of employment relationships and maintenance of learner records.

Where legitimate interests are relied upon, Carlow College carried out a legitimate interests test. This involves:

- Identifying a legitimate interest;
- Showing that the processing is necessary to achieve it; and

- Balancing it against the individual's rights and freedoms.

Where legitimate interests are relied upon as a legal basis for processing, the data subject is informed of the legitimate interests pursued by the controller or a third party at the time the data is collected. Data subjects have a right to object to processing carried out for legitimate interests.

Carlow College has a wide range of policies that affect employees and learners. The necessity of data processing and the management of personal data are either directly addressed or implied in these policies, which are to be read in conjunction with this Data Protection Policy and its Associated Documentation, and which will also be relied on as an assessment and statement of Carlow College's legitimate interests. College policies are formulated through documented, cross-functional and consultative means.

4.7 The concept of consent

Consent of the data subject is a complex concept. It is sometimes appropriate to seek consent to process personal data, and in other circumstances it may be unnecessary or inappropriate. The employment relationship is one area where it is considered that the concept of consent should not be used, due to the imbalance of power in the employer-employee relationship. Further information for employees on this topic is given in Data Processing at Work: Mechanisms Affecting Employees (Appendix 1).

Seek consent of the data subject to process his/her personal data, where it is required.

Consent mechanisms are set out in forms which are in use in Carlow College, where required. Employees are to comply with consent mechanisms that apply to personal data they handle. Data subjects may give consent verbally but written consent is preferred, where it is practical. The employee is to create a record if consent is given verbally.

'Explicit' consent is one of the legal bases on which the processing of special categories of data is permitted. The GDPR does not specify what action is required for explicit consent. It is recommended to employees that explicit consent should always be in a written format.

A sample consent form is given at Appendix 2. Employees may adapt this sample for use and are to consult the DPO prior to its use.

A number of conditions exist for obtaining valid consent. Employees are to note the following:

- The data subject may either give consent verbally or in writing;
- Consent must be verifiable (some form of record must be kept of how and when consent was given);
- The request for consent must be clearly distinguishable from the other matters in a written document. It must stand apart from other text;
- Prior to giving consent, data subjects must be informed of their rights to withdraw consent at any time and it must be easy for them to do so;

- Consent must not be sought in a contractual situation if the processing is not necessary for the performance of the contract (for example, requiring an employee to provide a photograph for an employer website as part of a contract of employment would not be proportionate).

Some other considerations:

- Consent must be sought for each different processing activity. If using tick boxes, have a tick box for each processing activity;
- Ticking a box when visiting a website or choosing technical settings for information society services (for example, online businesses) affirms consent;
- Silence, pre-ticked boxes or inactivity are not sufficient to constitute consent. If using tick boxes, they must be unticked;
- Consent is likely not valid where there is an imbalance of power between the controller and the data subject;
- Individuals have a stronger right to have their data deleted where consent is relied on as a legal basis for processing;
- Consent is not valid if the data subject has no genuine or free choice or cannot withdraw consent without detriment.

Carlow College seeks parental consent in writing in some instances where learners are under the age of 18, including Garda vetting and access to the College's Counselling Service. It is the responsibility of the responsible employee to seek and retain evidence of such consent.

4.8 Data subject rights and requests

Data subjects have a number of rights under the GDPR in terms of their personal data. They are:

- Right to information;
- Right of access;
- Right to rectification;
- Right to erasure;
- Right to restrict processing;
- Right to data portability;
- Right to object to processing;
- Rights in relation to automated decision making and profiling.

Many of these rights are not absolute. Restrictions are built into both the GDPR and national Data Protection legislation. Further information about these rights is available in the following sections.

Individuals also have various rights for remedies and liabilities, including,

- The right to lodge a complaint with supervisory authorities (Office of the Data Protection Commissioner in Ireland) where their data has been processed in a way that does not comply with the GDPR;
- The right to a judicial remedy against a relevant controller or processor; and
- The right to compensation from a relevant controller or processor for material or non-material damage resulting from infringement of the GDPR.

The supervisory authority applicable to Carlow College is the Officer of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois; info@dataprotection.ie; 1890 252 231.

4.9 Handling data subject requests

Data subjects may exercise their rights in respect of controllers. Requests must be in writing. A Data Subject Request Form is available at Appendix 3. A similar form CCTV Subject Access Requests is available at Appendix 4. Carlow College will seek verification of the identity of the requester prior to processing the request, where it is required.

Employees are to send Data Protection requests to the DPO for processing, without delay.

The following instructions and information is provided for employees:

- Any employee who receives a written Data Protection request is to send it to the DPO for processing without delay. The DPO will coordinate the reply to the data subject;
- Data Protection requests concern personal data. Requests for general information are not Data Protection requests but they may be Freedom of Information (FOI) requests. If a request is for information that would not normally be released or is not requested as part of everyday business, it is to be sent to the DPO. The DPO is also the FOI Officer. Any employee who is uncertain about the status of a request for information is to send it to the DPO;
- Data subject requests do not have to mention the GDPR or national Data Protection legislation. It is the duty of the controller to recognise Data Protection requests;
- Verbal requests are not Data Protection requests;
- Remember that a request may not just be for access. It may be for any of the rights listed in Section 4.8;
- Straightforward verbal requests for the updating of factual information eg new contact details of employee, learner or supplier are not Data Protection requests. Such requests should be handled by the responsible employees;
- The controller must reply to all data subject requests 'without undue delay' and 'at the latest within one month', although it is possible to extend this period in limited circumstances;
- The DPO will coordinate a reply to the request with the assistance of employees responsible for the data in question;
- Where a request is not complied with, reasons for the refusal must be given and the data subject must be informed of their right to complain to the supervisory authority and to a judicial remedy.

See also Section 4.11, which gives further information about the right to access.

Carlow College operates an informal mechanism whereby employees may have access to their employee file as held by the Human Resources Office and learners may have access to their student file as held by Academic Administration, without having to make formal Data Protection requests. Further information for employees is available in Data

Processing at Work: Mechanisms Affecting Employees (Appendix 1). Further information about handling learner records is available in Appendix 5.

Due to the complexity of the legislation, the following sections provide an overview rather than comprehensive treatment of data subject rights and the restrictions on same. Should employees require further information they may access the full text of the GDPR or seek clarification from the DPO.

4.10 Right of information

Tell data subjects that information about how Carlow College handles their personal data is available in our Privacy Notices.

Carlow College provides individuals with privacy information at the time that it collects personal data from them. Our Privacy Notices are available on the College website. Employees are to inform individuals of the existence and location of the Privacy Notices and this Data Protection Policy when seeking personal data. Depending on the circumstances, this may include:

- Giving individuals verbal information about the Privacy Notices with speaking or meeting with them;
- Giving a copy of the Privacy Notices to data subjects;
- Reference to the Privacy Notices in agreements and contracts;
- Reference to the Privacy Notices on forms, systems or webpages on which personal data is collected.

Where Carlow College obtains personal data from a source other than the individual to whom it relates, the responsible employee is to notify the individual within one month unless:

- the individual already has the information;
- providing the information to the individual would not be possible;
- or it would be disproportionate to do so.

Carlow College collects personal data directly from data subjects wherever possible, and limits collection of personal data from other sources.

If Carlow College plans to communicate with the individual the responsible employee will provide him/her with the Privacy Notices at the time of the first communication. If Carlow College plans to disclose the personal data to someone else, the individual will be informed by the responsible staff member, at the latest, when the data is disclosed.

4.11 Right of access

Individuals have a right of access to their personal data.

An individual has the following access rights with regard to a controller:

- To obtain confirmation as to whether his/her personal data is being processed;
- To access the data; and
- To be provided with supplemental information about the processing.

Carlow College requires to verify the identity of the applicant prior to the release of personal data. Where the access request is for visual data, such as CCTV, photographic identity is required.

Where the request is made in electronic form, the data will be provided electronically (unless the data subject requests otherwise). A copy of the information is provided free of charge. Where a controller holds a large quantity of data, it may ask the data subject to specify the information or processing activity to which the request relates.

The supplemental information that the controller is required to provide to data subjects correlates with that given in Privacy Notices. It includes, but is not limited to:

- The purposes of the processing;
- The categories of the personal data;
- The recipients or categories of recipients;
- The data retention period or the criteria used to determine this period;
- The individual's right of rectification or erasure, to restrict processing or to object to processing and to lodge a complaint to a supervisory authority;
- Details of any automated processing, including profiling; the logic involved, and the significance and envisaged consequences of the processing for the data subject; and
- Where the data are transferred to a third country or an international organisation, the appropriate safeguards, and how a copy of the safeguards can be obtained.

While individuals have a right of access to their personal data, there are some restrictions in place, for example, to health data where it may cause harm to data subjects; and information given on the basis that it would be treated in confidence.

Further information about employees and learners gaining access to their personal data is available in Appendices 1 and 5 respectively.

4.12 Right to rectification

Individuals have a right to have personal data rectified if it is inaccurate or incomplete.

Where a data subject requests rectification of his/her personal data and the controller complies, the controller must inform recipients to whom that data has been disclosed, unless this proves impossible or involves disproportionate effort. The controller must also inform the data subject about the recipients to whom the data has been disclosed if he/she requests it.

4.13 Right to erasure

Data subjects have a right of erasure of personal data, also known as 'the right to be forgotten'.

This applies in six scenarios:

- Where the personal data is no longer necessary in relation to the purposes for which it was collected;
- When the data subject withdraws his/her consent and there is no other legal ground for the processing;
- When the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- The personal data have been unlawfully processed;
- The personal data has to be erased to comply with an EU or Member State legal obligation; or
- The personal data has been collected in relation to the offer of information society services (online business) to a child. Carlow College does not offer information society services to children.

Where the controller complies with the request, the controller must take reasonable steps to inform other controllers to whom the data has been disclosed, of the request to erase any links to, copies or replications of, the personal data in question. This is challenging for controllers who process personal data in an online environment, for example, on social networks or websites. The controller must also inform the data subject about those recipients, if so requested.

There are grounds for a controller to refuse to comply with a request for erasure:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- The exercise or defence of legal claims.

4.14 Right to restrict processing

The right to restrict processing means that individuals can limit the way that organisations use their data.

A data subject's right to restrict processing applies in four scenarios:

- The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify its accuracy;
- The processing is unlawful, and the data subject opposes erasure and requests restriction instead;
- The controller no longer needs the personal data, but the data subject requires the data to exercise or defend a legal claim; or
- The data subject has objected to the processing. It should be restricted pending verification of whether the legitimate interests grounds or public interest tasks of the controller override those the rights of the data subject.

When processing is restricted, a controller is permitted to store the personal data but not to further process it. Where the data are processed automatically, the restriction should be effected by technical means and noted in the controller's IT systems. This could mean moving the data to a separate system; temporarily blocking the data on a website or otherwise making the data unavailable.

When a data subject exercises his/her right to restrict processing, the controller can only continue to process the data if:

- The data subject consents;
- The processing is necessary for the exercise or defence of legal claims;
- The processing is necessary for the protection of the rights of other individuals or legal persons; or
- The processing is necessary for public interest reasons under EU or Member State law.

Where a controller complies with a request to restrict processing, the controller has an obligation to inform recipients to whom that data has been disclosed, unless this proves impossible or involves disproportionate effort. The controller must also inform the data subject about those recipients if he/she requests it. The controller must notify the data subject before lifting a restriction. This is the responsibility of the employee who lifts a restriction.

4.15 Right to data portability

The right of data portability enables individuals to obtain their data, and have it transmitted to another controller, where technically feasible.

The right only applies to personal data an individual has provided to a controller. It does not include data generated by a controller.

The right to data portability only applies where:

- The processing is based on the data subject's consent or for the performance of a contract; and
- The processing is carried out by automated means.

4.16 Right to object to processing

The GDPR does not provide a general right for a data subject to object to processing. Data subjects have a right to object to:

- Processing based on public interest, official authority or legitimate interest grounds (including profiling based on those grounds)
- Direct marketing (including related profiling); and
- Processing for scientific, historical research or statistical purposes (unless the processing is necessary for the performance of a public interest task).

Where a data subject objects to processing carried out for the performance of a legal, public interest or official authority task or legitimate interests, the controller must stop processing the personal data unless the controller demonstrates:

- Compelling legitimate grounds for the processing which override the rights of the data subject; or
- The processing is necessary for the establishment, exercise or defence of legal claims.

Objection to the processing of personal data for direct marketing purposes is an absolute right.

Appendix 6 comprises Guidelines for Employees: Marketing and Publicity.

Where an objection to research is made, individuals must have 'grounds relating to his or her particular situation' in order to exercise their right to object. Employees and learners conducting research should pseudonymise or anonymise personal data wherever possible in order to reduce risk to data subjects. Pseudonymised data is personal data and is subject to the GDPR, but anonymised information is not. Where research is necessary for the performance of a public interest task, it is not required to comply with an objection to processing.

The right to object must be explicitly brought to the attention of the data subject, at the latest at the time of first communication with him/her and must be presented clearly and separately from other information.

4.17 Rights in relation to automated decision making and profiling

The GDPR applies to all automated individual decision making and profiling (automated processing to evaluate certain things about an individual).

For example, the following may constitute automated individual decision making and/or profiling:

- Use of an electronic system to tally learner grades;
- Use of an electronic system to calculate employee attendance;
- Systematic collection of data about visitors to a website;
- Online behavioural advertising; and
- An aptitude test which uses pre-programmed algorithms and criteria.

Automated decision making does not have to involve profiling, although it often does. The GDPR provides a right for data subjects not to be subject to a decision based solely on automated processing, including profiling, which produces a legal effect or other similarly significant effect on him/her.

The restriction on automated processing does not apply if the decision is:

- Necessary for the performance of a contract between the data subject and controller;
- Authorised by EU or Member State law; or
- Based on the explicit consent of the data subject.

However, suitable safeguards must be in place to protect the person's interests.

Where Carlow College utilises automated processing and profiling, the responsible employees must ensure that if the decision will have legal or other significant effect on an individual, that they check and verify the data for accuracy on request. Individuals must be able to easily request human intervention, for example, learners must be able to request that a human verifies

Where profiling occurs on the basis that it is necessary for the performance of a contract or with the explicit consent of the data subject, the data subject must be given 'at least the right' to express his/her point of view and to contest the decision. All processes must be fair to data subjects.

There is a restriction on profiling using special category data unless the data subject has given explicit consent, or it is necessary for public interest reasons. Controllers must inform data subjects at the time data is obtained, of the existence of profiling (that is, purpose) involved, as well as the significance and consequences of such processing for the data subject.

Regular checks must be carried out to ensure that automated processing systems are working as intended. This includes quality checking the data therein. These controller obligations are the responsibility of operational staff.

4.18 Data Protection by Design and by Default

The GDPR includes the concepts of privacy by design and by default, which have the objective of embedding data protection considerations into processing operations during the design phase, rather than as an after-thought.

Privacy by design requires controllers to implement appropriate safety mechanisms (technical and organisational measures) to ensure that, by default, processing is achieved by the most privacy friendly method possible.

When deciding on what technical and organisational measures are appropriate, the controller must take the following into account:

- The state of the art;
- The cost of implementation;
- The nature, scope, context and purposes of processing; and
- The risks of the processing to individuals' rights.

Thus, not all personal data is subject to the same technical and organisational measures. Employees must consider Data Protection issues at an early stage in project design. They may find it useful to consult with the DPO. Data Protection Impact Assessments, described in the next section, are useful tools to effect privacy by design and by default.

4.19 Data Protection Impact Assessments (DPIAs)

DPIAs assist controllers to identify problematic issues at an early stage in the design of projects and processing operations involving personal data, and to address problems in order to comply with Data Protection legislation, reduce risk and reputational damage which might otherwise occur.

DPIAs are compulsory under the GDPR where processing begins after 25 May 2018 and are likely to result in 'high risk' to the rights of individuals, taking into account the nature, scope, context and purposes of the processing. The precise meaning of 'high risk' has not been defined in the GDPR and is open to interpretation.

DPIAs must be carried out when:

- Using new technologies; and
- The processing is likely to result in a high risk to the rights and freedom of individuals.

Processing that is likely to result in a high risk includes, but is not limited to:

- Systematic and extensive processing activities, including profiling and where decisions have legal effects, or other similarly significant effects, on individuals;
- Large scale processing of special categories of data, including data relating to criminal convictions or offences;
- Large scale, systematic monitoring of public areas (CCTV).

Employees are to consider if a DPIA would be beneficial or required in terms of projects or tasks that they undertake. Employees are to contact their line manager for further information about DPIAs.

Carlow College will carry out DPIAs where advisable or required. It is the responsibility of operational employees and line managers to give consideration to the use of DPIAs in their tasks and projects. The GDPR requires a controller to seek the advice of its DPO when carrying out a DPIA.

There is no defined format for a DPIA but the GDPR sets out the minimum information which it should contain:

- A description of the proposed processing activities; their purpose, and the legitimate interest pursued by the controller;
- An assessment of the necessity and proportionality of the processing activities in relation to the purpose;
- An assessment of the risks to the rights of data subjects; and
- An assessment of the risks, safeguards and security measures proposed to be taken to demonstrate compliance with the GDPR.

The DPIA should be reviewed, at a minimum when there is a change of the risk in the processing operations. This is the responsibility of the relevant line manager.

Prior consultation with the Data Protection Commission is required where a DPIA indicates that the processing would result in a 'high risk' to individuals despite the implementation of safety measures. This should be a rare occurrence.

4.20 Obligations on Processors and Contracts with Processors

Carlow College is a controller for most of the personal data that it processes. In some instances, the College is a processor or the College engages processors. This section is applicable in both explaining the College's obligations as a processor and considerations to be taken into account when engaging a processor. Under Article 28 of the GDPR controllers are obliged to agree contracts with processors which process personal data on their behalf.

Where any employee requires to engage a processor he/she is to inform the DPO in advance of execution of any type or contract or service agreement, and additionally, to inform the IT Officer where the processing of data utilises an electronic device, IT systems or online resources, in order to ensure that technical security is adequate.

Agreement of contracts is the responsibility of relevant line managers.

Carlow College must only engage processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subject protected.

The GDPR imposes specific obligations in regard to the terms of a data processing contract. The following terms are mandatory under Article 28:

- To process data only on documented instructions from the controller;
- To ensure that the processor's staff are committed to confidentiality;
- To take all appropriate security and organisational measures;
- To sub-contract only with the prior permission of the controller;
- To assist the controller in complying with the rights of the data subject;
- To assist the controller in complying with its obligation, including DPIAs and data breach notifications;
- To delete or return all personal data to the controller, if requested, at the end of the processing; and
- To make available to the controller all information necessary to demonstrate compliance with its processing obligations and allow audits to be conducted by the controller.

Employees must familiarise themselves with the terms of any contract or data sharing agreement that is in place for personal data they process. Employees must ensure that they abide by terms of such contracts or data sharing agreements.

The GDPR limits the liability of processors to a certain extent, by providing that they will only be liable for damage caused where they have not complied with processor-specific obligations in the GDPR or if acting outside the instructions of the applicable controller. Contracts should also ensure appropriate risk allocation for data breaches between controllers and processors. It is inevitable that there will be litigation on the issue of causation in the context of a data breach in light of the provision in the GDPR permitting joint liability for breaches.

Processors must keep a record of their processing activities and notify personal data breaches to controllers.

4.21 Joint Controller Agreements

Where two or more controllers jointly determine the purposes and means of processing, they are joint controllers and must have an arrangement in place outlining their respective responsibilities under the GDPR.

Where any employee requires to make an agreement with a joint controller he/she is to inform the DPO in advance of beginning processing, and additionally, to inform the IT Officer where the processing of data utilises an electronic device, IT systems or online resources in order to ensure that technical security is adequate. The execution of suitable arrangements with joint controllers is the responsibility of relevant line managers.

Again, employees are to familiarise themselves with any agreement with a joint controller that affects personal data they process and ensure compliance with it.

4.22 International Data Transfers

The GDPR imposes restrictions on the transfer of personal data outside the EU, to third countries or international organisations. The restrictions are in place to ensure that the level of protection given by the GDPR is not undermined. Various mechanisms for transfer are set out in Chapter V of the GDPR.

Employees who require to transfer personal data outside the EU are to discuss the matter with their line manager prior to transfer.

The Privacy Notices and Records of Processing Activities set out arrangements that Carlow College has in place. Where any employee requires clarification, or if a new arrangement requires to be implemented, he/she is to contact the DPO to discuss the matter.

There are various mechanisms which it is possible to use for international data transfer. It is emphasised that international data transfers are in a state of flux at present as there are legal challenges pending in some areas.

Adequacy Decisions under Article 45 of the GDPR. The EU Commission is the authority which decides that a third country or specified sector within that country or international organisation ensures an adequate level of protection. Transfers of data to such countries will not require specific authorisation, for example, data transferred from the EU to the US using the Privacy Shield mechanism. US organisations which are signed up to Privacy Shield are listed at www.privacyshield.gov.

Appropriate Safeguards under Article 46 of the GDPR. The GDPR permits transfers to third countries where 'appropriate safeguards' are in place, such as Model Clauses.

Derogations under Article 49 of the GDPR. The GDPR permits transfers to third countries in specified situations including, but not limited to the following:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- The transfer is necessary for the performance of a contract between the data subject and the organisation or the implementation of pre-contractual measures, taken at the data subject's request;
- The transfer is necessary for the performance of a contract made in the interest of the data subject between the controller and another legal person;
- The transfer is necessary for important reasons of public interest;
- The transfer is necessary for the establishment, exercise or defence of legal claims;
- The transfer is necessary in order to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent. This would include a life or death situation;
- The transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation.

4.23 Personal Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Any employee who becomes aware of an actual or suspected personal data breach, or that data has been placed at risk, is to notify the DPO without delay. This includes notification to an employee by any processor or joint controller of Carlow College of any such incident.

The communication to the DPO is to be made by telephone or in person. Email is not acceptable due to the promptness required in responding to breach situations. If the employee does not succeed in contacting the DPO, he/she is to contact the Office of the President, the Director of Operations or his/her line manager, in that order, without delay.

There are three types of breaches:

- **Confidentiality breach** – where there is an unauthorised or accidental disclosure of, of access to, personal data;
- **Availability breach** – where there is an accidental or unauthorised loss of access to, or destruction of, personal data;
- **Integrity breach** – where there is an unauthorised or accidental alteration of personal data.

A breach can involve a combination of the above.

The following are examples of what may constitute breaches or should be investigated to ascertain if a breach has occurred:

- Sending personal data to an unintended or unauthorised recipient, either internal to the College or external;
- Loss or theft of a paper file, memory stick, removable device or laptop;
- Unauthorised destruction or unauthorised alteration of personal data;
- An attack on IT systems;
- Attacks on physical security, for example, forcing of doors, windows or filing cabinets;
- Disposal of personal data in an unsecure manner;
- Failure to effectively wipe electronic devices;
- Where a system containing personal data is 'down' and is not accessible.

Most personal data breaches arise from human error rather than deliberate action such malicious attacks on IT systems, which receive more attention because of the large numbers of data subjects often affected.

It is emphasised to employees that it is better to report any situation that may constitute a breach immediately in order that it can be contained and dealt with as quickly as possible. Breaches can cause serious reputational damage for organisations, and the GDPR provides for both administrative fines and the possibility of data subjects making claims for compensation. Timely and effective response to breaches leads to fewer negative consequences for organisations.

Carlow College's Personal Data Breach Response Plan is set out at Appendix 7.

4.24 Audits of Data Protection Practices

The DPO will carry out audits at regular intervals. All employees are to comply with Data Protection audits. The DPO will submit Data Protection audit reports to relevant employees and their line managers for review. Reports are submitted by the DPO to the President.

4.25 Archival Records

The long-term retention of personal data for purposes of archiving in the public interest, scientific or historical research or statistical purposes is alluded to at various points in the GDPR. Such archiving is to be subject to suitable safeguards to protect the rights and interests of data subjects.

The archival records of Carlow College are cared for by the Delany Archive, an independent charitable trust, which is housed in Carlow College. A separate suite of policies applies to the management of the Delany Archive.

Safeguards which are in place include:

- The closure of documents to research for suitable periods;
- The closure of documents to research until they have been catalogued;
- The marking of documents with identification codes;
- The registration of researchers;
- Restrictions on the reproduction and distribution of documents;
- The supervision of researchers in the Reading Room;
- Physical access controls within the Archive;

- Written deposit agreements with owners of collections;
- Written policies and procedures;
- Pseudonymisation will be carried out, where appropriate.

5. Roles and Responsibilities

5.1 Controller (President, Carlow College)

The controller has a wide range of responsibilities under the GDPR and national Data Protection legislation;

The responsibilities of controllers and processors towards their DPOs are set out in Article 38 of the GDPR. In accordance with this, Carlow College's obligations towards its DPO are the following:

- Carlow College will ensure that the DPO is involved, properly and in a timely manner in all issues which relate to the protection of personal data;
- Carlow College will support the DPO in performing his/her tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his/her expert knowledge;
- Carlow College will ensure that the DPO does not receive any instructions regarding the exercise of those tasks. The DPO will not be dismissed or penalised by Carlow College for performing his/her tasks.

Carlow College acknowledges that data subjects may contact the DPO with regard to all issues relating to processing of their personal data and to the exercise of their rights under the GDPR. Carlow College further acknowledges that the DPO is bound by secrecy or confidentiality concerning the performance of his/her tasks, in accordance with EU or Member State law.

5.2 Managers

- It is the responsibility of relevant Managers to develop and encourage adequate and responsible data and records handling practices within their areas of responsibility;
- Managers are obliged to ensure the DPO is informed in a timely manner of Data Protection issues.

5.3 All employees

- All employees who process personal data are required to abide by this Policy and Associated Documentation, both now existing and introduced in the future;
- Employees are to handle queries about personal data in a courteous and efficient manner;
- Employees are obliged to ensure that the DPO is informed in a timely manner of Data Protection issues;
- Employees are to cooperate with the DPO in the exercise of his/her tasks;
- Employees are responsible for adherence with data sharing agreements and contracts pertaining to their area of work;
- Employees are to avail of training where it is made available to them;

- Failure to abide by this Policy and Associated Documentation may result in disciplinary action, up to and including dismissal.

5.4 Data Protection Officer (DPO)

The DPO of Carlow College has the following tasks in accordance with Article 39 of the GDPR:

- To inform and advise Carlow College and its employees who carry out processing of their obligations pursuant to the GDPR and other Data Protection legislation;
- To monitor compliance with the GDPR and other data protection legislation; and with the policies of Carlow College in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits;
- To provide advice, where requested, as regards DPIAs and to monitor their performance pursuant to Article 35 of the GDPR;
- To cooperate with the Office of the Data Protection Commissioner;
- To act as a contact point for the Office of the Data Protection Commissioner on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate with regard to any other matter;
- The DPO will act as a liaison with the Office of the Data Protection Commissioner in connection with personal data breaches, when requested by Carlow College;
- The DPO shall in the performance of his/her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

The DPO will coordinate responses on behalf of Carlow College to data subjects exercising their rights under the GDPR and other Data Protection legislation. The DPO reports to the President. The DPO is bound by secrecy or confidentiality concerning the performance of his/her tasks, in accordance with EU or Member State law.

6. Associated Documentation

Privacy Notices

7. Appendices

1. Data Processing at Work: Mechanisms Affecting Employees
2. Sample consent form
3. Data Subject Request Form
4. CCTV Subject Access Request Form
5. Handling Learner Records
6. Guidelines for Employees: Marketing and Publicity
7. Personal Data Breach Response Plan
8. Rules for Employees: Safeguards to Protect Personal Data

8. Referenced Policies

Records Management Policy

Freedom of Information Policy

Garda Vetting Policy

Policies of the Delany Archive

Disciplinary Policy

9. Monitoring and Review

Data Protection is an evolving area and this Policy will be kept under continuous review by the DPO.

10. Disclaimer

This Policy does not purport to be an accurate or exhaustive interpretation of the GDPR or national Data Protection legislation.

11. Appendices

1. Data Processing at Work: Mechanisms Affecting Employees

Introduction

Employers process a significant amount of personal data about employees. The purposes of this document are:

- To introduce Data Protection and privacy issues in the Carlow College, St. Patrick's (hereafter Carlow College) employment context, and the interests, rights and obligations of both employer and employees;
- To outline some mechanisms associated with records and data management.

This document is an Associated Document of Carlow College's Data Protection Policy and is further informed by that Policy.

General principles

- Carlow College processes a range of personal data types about employees;
- Personal data is defined in the GDPR as any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a person;
- Names, email addresses, car registration information, photographs, letters regarding health appointments and GPS data on a phone are, or may be, examples of personal data;
- Where the word 'employee' is used in this document it is intended to cover all situations where there is an employment relationship, regardless of whether the relationship is based on an employment contract, a volunteer agreement or a contract for services etc;
- Employees can assume reasonable privacy expectations at work;
- Employers have a legitimate interest in processing personal data about their employees or may have obligations, such as under legislation, to process such data.

The concept of consent at work

- Previously, employee data was often processed by employers on the basis of employee consent;
- Under the GDPR, there are a range of legal bases that employers may use to process personal data and special categories of data. The latter were known as 'sensitive personal data' under the Data Protection Acts 1988 and 2003 and now incorporate data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or orientation;
- Due to nature of the employment relationship and the strictures of the consent mechanism, consent is often not a prudent or possible basis on which to process employee data. In part, this is due to the imbalance of power in the employer-employee relationships. Employees may feel pressured to give consent for processing where they may prefer not to;

- Controllers such as employers can use a range of legal bases to process personal data. These are set out in Article 6 of the GDPR. The legal bases for processing special categories of personal data are set out in Article 9 of the GDPR. Article 6 includes, for example, that an employer may process personal if there is a legal obligation on them. For instance, employers require to hold certain information to comply with Workplace Relations Commission inspections; and employers are required to carry out risk assessments in respect of expectant mothers under health and safety law. In situations such as these, employers should not ask for consent to process the personal data. Consent would not be valid because the data subject does not have free choice in such matters and may suffer detriment if the processing stopped;
- As a result, Carlow College will seek employee consent to process personal data where it is necessary, but otherwise, will seek to use the bases laid out in Articles 6 and 9 of the GDPR. To seek consent where the conditions of the consent mechanism cannot be fulfilled would not be fair to employees.

<u>Requests under the GDPR by employees</u>

- Where employees are data subjects, they have the same rights as data subjects in all other situations as are provided by the GDPR;
- Personal data about employees may be held by a number of College offices, appropriate to their functions. In terms of information regarding and arising from contracts of employment, the general policy is that this data is centralised in the Human Resources Office. Line managers may hold a copy of some data, as appropriate. Leave Administration holds records regarding employee leave and attendance, including supporting documentation such as medical certificates. Personal data is shared with or collected by the Accounts Departments as required for payroll and other relevant purposes, including taxation, social welfare and expenses. Where the Accounts Departments holds authorisations issued on or behalf of employees to deduct trade union dues from their wages/salary, such authorisations are held with the explicit consent of the employee and are used for no other purpose by Carlow College, St. Patrick's. The Accounts Department does not share trade union membership data that it holds with other departments and offices. Employee data protection requests regarding trade union data held by the Accounts Department will be handled in the Accounts Department and/or in consultation with the DPO;
- This information is outlined for employees by way of explanation that human resources records and what is traditionally called an 'employee file' may be held in both physical and electronic formats, across several offices, appropriate to their functions;
- In general, Carlow College operates an open access policy for employees who wish to view their 'employee file', as held by the Human Resources Office. In general, employees do not have to submit a formal subject access request to exercise their right of access, but if so wished, employees may submit subject access requests to the DPO;
- Where employees wish to access a range of records wider than the content of the 'employee file' held by the Human Resources Office, they are requested to submit a formal subject access request to the DPO in order to facilitate accurate retrieval of requested data;
- Employee access requests will be fulfilled as quickly as possible. Employees should appreciate that in some instance their human resources records may contain references to other natural persons. Data subjects are entitled to access their own personal data only. Therefore, records must be checked for third party data prior to giving access to employees. Third party data will be redacted.

- Access to health data may be restricted if it would be likely to cause serious harm to the physical or mental health of the data subject. For the information of employees, health records may be held by the Occupational Health Provider (OHP) contracted by Carlow College, St. Patrick's. Where employees undergo medical examinations at the request of the College with the OHP, the only information released to the College is whether or not the OHP considers the employee medically fit to carry out their duties. The College provides the employee's job description to the OHP in order that it can used to determine employee fitness. Employees may apply for access to their personal data held by the OHP;
- Data subjects have rights other than access under the GDPR. They are information, rectification, erasure, portability, restriction and objection. The information right is met by the Privacy Notices, but further information will be made available where possible. Where an employee wishes to exercise the other rights, they are requested to apply to the DPO in order that the request can be processed formally.

Mechanisms affecting IT Services and manual records

New employees: access permissions

- The Human Resources Office will inform the IT Officer when a new employee is to commence employment in order to permit the IT Officer to set up required accounts and grant access to various electronic systems;
- The IT Officer will liaise with the new employee's line manager to ensure that the correct access permissions are granted, based on the new employee's duties. Access permissions will be adequate, relevant and not excessive;
- The Human Resources Office is also to inform Reception staff of a new employee's details (name, mobile phone number and position) where the new employee has consented to being added to the College's text messaging system. The text messaging system is accessible to a small number of authorised employees only and is used to communicate important and urgent messages to employees and learners. If employees do not consent to receipt of text messages they may not receive important information in a timely manner;
- The line manager will ensure that the new employee has access to required physical records in order to permit the carrying out of assigned duties, and that this access will be adequate, relevant and not excessive.

Existing employees: internal transfers

- Employees who change position within Carlow College are to transfer all records pertaining to their former duties to either their successor or their current line manager. It is the responsibility of the current line manager to ensure that this handover occurs;
- The IT Officer and both the current and new line managers, if they are different, will liaise in order to ensure that the correct access permissions are granted to the employee based on their new duties. This may involve the removal and/or granting of access permissions;
- Should the employee's new duties be unrelated to their former duties, they should not retain in their personal custody the personal data of other persons held by virtue of their former duties or more general records that are of ongoing value to other colleagues.

Departing employees

- Employees who leave the employment of Carlow College are to leave all official records for their successor. It is the responsibility of the line manager to ensure that records remain with the College;
- Employees are not to remove any records owned by Carlow College without the prior written authorisation of their line manager;
- Employees are not authorised to delete or destroy records covered under the Records Retention Schedules without prior written authorisation under the Records Destruction Procedure;
- On the day that employment ceases, the IT Officer will deactivate the employee's email account and access permissions, take custody of the employee's computer, back up the contents of the computer and wipe it by restoring it to factory settings. Departing employees are to take with them, before employment ceases, records in either manual or electronic formats which are their personal property. It may not be possible to provide such access after employment ceases.

Management changes and personal data

- Where the line management structures of an employee change, the former line manager is to liaise with the Human Resources Office to identify records of continuing validity and importance. Such records should be transferred to the Human Resources Office or the new line manager, as appropriate, in order to ensure continuity;
- The former line manager is to apply to destroy expired use records in accordance with the Records Destruction Procedure. Employees should not continue to hold records pertaining to persons they no longer manage.

Employer access to records and data

IT resources are provided to employees primarily to enable them to carry out the official business of the College, for which they are contracted. Employees are permitted a limited amount of personal use of IT resources. Typically, employees might use their work email account or create personal documents using word processing software for private, personal communications. Employees can have reasonable privacy expectations at work and employers have a legitimate interest in securing and having access to their assets, including information. Under Carlow College's contracts of employment and Records Management Policy, all records created and received by employees in the course of conduct of their official duties are the property of the College.

Employees should be cognisant that Carlow College may require access to information in employee network accounts, including email accounts and records in other formats. The following statements apply equally to records in all formats, including paper records.

Except in exceptional circumstances, existing employees will be notified of a requirement to access their accounts. An example of an exceptional circumstance is a criminal investigation. Such situations would be discussed by line management, senior management, the IT Officer and the DPO, as appropriate. Where the accounts of existing employees are accessed without prior notification, employees will be informed about the access at the earliest opportunity that presents itself. Only required information will be accessed.

Employees should also be cognisant that the employer may have a requirement to access their accounts following the termination of the employment relationship. Again, such access requirements will be discussed by line management, senior management, the IT Officer and the DPO, as appropriate. Only required information will be accessed.

Employer access to accounts is also relevant when existing employees are absent from work and access to information in their accounts is required for legitimate business purposes. The following mechanism is put in place in order to permit required access to accounts in a manner that is fair and transparent to both employer and employee. All situations will be considered on a case by case basis and the following steps are not prescriptive. Every situation will be handled in the least intrusive manner possible. Steps additional to the following may be required:

- If an employee is absent and the need to access information in the account is urgent, in the first instance, the line manager will contact the employee, if possible, to ascertain if the employee can forward the required information;
- If this is not successful, the line manager may apply to the IT Officer in writing for access to the account;
- Access requests from employees who are not in a line management relationship with the account user will not be granted;
- The line manager should specify to the IT Officer: when the employee is expected back at work; the reason for requiring access; for what period access is required;
- Wherever possible, the line manger should access the account him/herself and access only the required information;
- If the line manager requires to reply to emails he/she should forward them to his/her own account so that the reply comes from the line manager's profile and copy the message to the absent employee's account, if appropriate;
- Under no circumstances is an employee to impersonate another employee by signing him/herself as the absent employee;
- Depending on the length of the expected absence, it may be prudent for the line manager to add an 'out of office' notification to the account and direct future email senders to a different recipient;
- The line manager should inform the employee about the accessing of the account on his/her return to work, at the latest.

Employees who are aware that their absence may be of some duration or who are aware that important emails may be received in their accounts should activate 'out of office' messages prior to their departure and notify important correspondents of a colleague's contact details. Employees who are aware that other employees may require access to information in their accounts during their absence, should, where possible, transfer such information to a colleague.

Social media

This issue is primarily treated of in the College's Social Media Policy (forthcoming), and that Policy should be read in conjunction with the information outlined here. There is some intersection between Data Protection and social media and it is appropriate to include comment here.

The advent of social media has created a blurred line between professional and personal affairs in some instances. Many persons can be seen to use the same profiles for these dual purposes. The College's official social media accounts are subject to the GDPR and this Policy. The GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and with no connection to a professional or personal activity. Personal or household activities could include correspondence and the holding of

addresses, or social networking and online activity undertaken with the context of such activities.

Carlow College should not and does not systemically or otherwise monitor the personal social media accounts of employees. The College recognises that employees are entitled to their privacy. However, that does not preclude the possibility of such accounts being brought or coming to the attention of the College as an employer. Employees are reminded that social media postings may be deemed to be in the public domain rather than private, and social media users are responsible for their online content.

Employees are contractually bound to maintain the confidentiality of College information and records, including personal data. Employees are not to reveal, discuss or compromise the integrity, security or confidentiality of personal data or other information about College business obtained during the conduct of their duties, in their social media use. Employees are to respect the dignity and privacy of colleagues, learners and other College stakeholders in their social media use. Employees are to obtain the permission of work associates before posting images or information about them online. Contraventions of employees' contractual duty of confidentiality and obligations under the Data Protection Policy will be treated very seriously by Carlow College and may result in disciplinary action up to and including dismissal.

2. Sample consent form

Carlow College, St. Patrick's

Keep in touch with us! Our events and services might interest you. We are a third level college and provide courses in the areas of Humanities, Social Care and Community and Citizenship. We organise public lectures and conferences on related topics.

Please fill in the contact details you want us to use to keep in touch with you:

Name

Address

Email

Telephone number

Please tick the boxes to tell us what you would like to receive information on:

□ Humanities courses

□ Social Care courses

□ Community & Citizenship courses

□ Public lectures and conferences

Please tick the boxes to tell us all the ways you are happy to hear from us:

□ Yes, I would like to receive communications by email

□ Yes, I would like to receive communications by telephone

□ Yes, I would like to receive communications by text message

□ Yes, I would like to receive communications by post

By signing this form you are consenting to Carlow College, St Patrick's contacting you for the indicated purposes.

Signature

Date

You can find out more about how we use your data in our Privacy Notices which are available on our website. You can grant consent to none, some or all the purposes. You can withdraw or change your consent at any time by contacting the Marketing Office, Carlow College, St. Patrick's, College Street, Carlow; or marketing@carlowcollege.ie; or 059-9153200. We will stop processing your personal data for this purpose once you have withdrawn consent, but this will not affect the lawfulness of processing prior to the withdrawal of consent. We will not share your data with any third party.

3. Data Subject Request Form

You can use this form to make a request under the GDPR.

We need to verify your identify in order to process your request. Please include a form of identification (eg passport, driver's licence, student ID card). This must take the form of photo-identification if you are requesting access to visual records.

Please include details we can use to easily contact you if we need further information to process your request.

Requests may be sent to the Data Protection Officer, Carlow College, St. Patrick's, College Street, Carlow; dataprotection@carlowcollege.ie; 059-9153200

We will reply as quickly as possible, and within one month.

Data subject contact details:

Name

Address

Email

Phone No.

Data subjects have number of rights under the GDPR. Please tick those rights which you are exercising:

□ Right to information
□ Right of access
□ Right to rectification;
□ Right to erasure;
□ Right to restrict processing;
□ Right to data portability;
□ Right to object to processing;
□ Rights in relation to automated decision making and profiling.

Please tell us what personal data forms the basis of your request and give us any further information we might need.

4. CCTV Subject Access Request Form

Where a person is identifiable in CCTV images, it constitutes personal data and a copy of the images may be requested from the controller.

We must verify your identity. Please include a copy of recently-issued photo-identification with your application so that we can recognise you in our CCTV footage (for example, driver's licence, passport, student ID card). Images of third parties will be redacted.

Please include contact details where we can easily reach you in case we need further information to process the application.

Applications may be submitted to the Data Protection Officer, Carlow College, St. Patrick's, College Street, Carlow; or dataprotection@carlowcollege.ie; or 059-9153200.

We will reply to you as quickly as possible, and within one month.

Name
Address
Phone number
Email address

To help us locate the relevant footage, please provide as much detail as possible:
Date
Time
Location
Description of incident

5. Handling Learner Records

Access requests by learners

Learners may access their own file, as held by Academic Administration, without submitting a formal written Data Protection access request;

Academic Administration is to verify the identity of the learner prior to giving access to personal data;

Academic Administration is to check through the file prior to giving access to the learner to ensure that it does not contain:

- Third party information, which should be removed or redacted, as appropriate
- Restricted information, which might include information regarding physical or mental health whose release may cause serious harm to the learner. Where a file contains such data, the learner's request is to be sent to the DPO;

Learners may view the file in the Academic Administration office and may request copies of documents;

Where learners request access to personal data held in other offices in the College, or wish to exercise a right other than access, they should do so on the basis of a formal Data Protection request in order to facilitate full consideration of the request.

Releasing learner information to family members

- In most circumstances, Carlow College cannot release information about learners to parents/guardians and other family members without the consent of the learner;
- Only in limited circumstances, such as a medical emergency, can the College release such information without consent.

6. Marketing and Publicity: Guidelines for Employees

Introduction

- These guidelines are for the use of employees of Carlow College, St. Patrick's (hereafter Carlow College) who carry out marketing and publicity functions. These guidelines respect the rules set down by the General Data Protection Regulation (GDPR) and other Data Protection legislation;
- Further legislation is this area is due in the form of a new ePrivacy Regulation (European Union; hereafter EU). A draft text only is available and it is unclear when this legislation will be implemented. It includes the same concepts as the GDPR but may impose further strictures;
- This is an Associated Document of Carlow College's Data Protection Policy. Information in that Policy further informs that given here.

Direct marketing

Direct marketing refers to the promotion of aims and ideals as well as goods and services.

Postal marketing

- For mail to be considered to be direct marketing, it must, generally speaking, be addressed to a named person and must be promoting a product or service. Unaddressed mail or mail addressed to 'the occupant' or 'the householder' does not normally use personal data, and consequently, data protection legislation does not apply. However, if an address is included, and the controller can identify 'the occupant' or 'the householder', data protection legislation would apply;

- Rules do not normally apply to postal marketing of corporate entities (eg companies) including marketing of office holders within such an entity (eg Careers' Guidance Counsellors in schools) provided that the marketing is related to the organisation's business needs and that the details of the named person were fairly obtained. However, if a person opts out you must respect his/her wishes and stop direct marketing.

Some current rules

- The rules in this document (https://www.dataprotection.ie/docs/DIRECT-MARKETING-A-GENERAL-GUIDE-FOR-DATA-CONTROLLERS/905.htm), from the Office of the Data Protection Commissioner's website continue in force at the moment. This document may change when the new ePrivacy Regulation is implemented;
- The document includes a useful table when opt-in and opt-out mechanisms are appropriate;
- Opt-out means that you can market an individual provided you have previously given them the option not to receive such marketing and they have not availed of this opportunity;
- Opt-in means that you can only market an individual where you have their explicit consent to do so;

- It should be noted that these rules provide for a 'soft' opt-in mechanism. It applies to commercial marketing of goods and services to existing customers. As a registered charity, Carlow College does not use the 'soft' opt-in mechanism;

- Some marketing guidance directed to charities refers to charities that seek donations for their charitable works. However, as a registered charity should the College direct such a campaign for any charitable purpose care should be taken to ensure compliance;
- Direct marketing does not include marketing that is made available to individuals generally eg if all visitors to a website see an advertisement. However, online behavioural advertising is subject to Data Protection.

The concept of consent

Consent of the data subject is defined in the GDPR as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her;

Gaining consent for direct marketing

- A sample consent form is available at Appendix 1;
- When seeking consent, you should be able to identify the:
    - Name or other identifier of the individual eg email address;
    - The date that consent was given;
    - The platform or mechanism you used to gain consent eg phone call; email; web form; manual form;
- If you are compiling marketing contacts lists in spreadsheets or other software from various sources, ensure that you capture the aforementioned data;
- Consent may be verbal;
- Exactly what the consent covers eg to send information about courses; or to send information about events held in Carlow College;
- It is not permissible to seek a general consent for 'marketing purposes'. Consent must be specific so that the person is adequately informed as to what he/she is consenting;
- Consent must be a positive action that makes it clear that the individual consents to the use of his/her information for marketing;
- Pre-ticked opt-in boxes are not permitted;
- Opt-out statements are not to be used;
- Consent statements must be plainly worded. Confusing language should not be used;
- Silence or inactivity from the data subject will not constitute consent;
- Ensure that consent for marketing is 'unbundled' from other requests for consent. For example, if you happened to need consent to share information with a third party, there would have to be two consents sought, one for the marketing and one for the information sharing;
- Ask individuals what method(s) of communication they would like used to communicate with them eg email, text, phone call, post. Have a tick box for each. Don't offer a method of communication if you don't intend to use it;
- Be non-prescriptive in the way that you seek information so don't make fields 'required' on forms. It is better to use a phrase such as 'Please fill in the contact details that you wish us to use to keep in contact with you';
- You should 'archive' the text of the website, leaflet, form, leaflet, contract etc which you used in conjunction with the consent. You should cross reference this information with consent records to enable you to have an accurate record of what was consented to if you need to retrieve it;
- If you pass the details of individuals to third parties for marketing purposes, then you must specifically request this consent. You must provide the individual with the name

of any and all of the third parties. It is recommended that Carlow College should not give its marketing contact lists to third parties;

- If you are offering online services to children and you need to obtain consent, you must adopt age verification measures and seek parental consent for children under the age of 13;
- You should determine a timeframe for how long consent 'endures'. This is not covered in legislation but one year is recommended for now as a maximum timeframe, in general. However, for individuals who express an interest in attending academic courses in the College it would be difficult to justify retention of their contact details past the following October as they will likely have taken positive action at that point if they wish to become a Carlow College student. It is suggested that such contact details should be deleted at that point or ask individuals to reconsent. If there is a mailing list of individuals interested in attending public events such as lectures and exhibitions, consent might endure for a year before you seek fresh consent;
- Depending on how they are structured, you may need to ensure that the format in which you record your marketing contacts lists are sortable by date so that you are identify data of individuals at the time for reconsent;
- Electronic mail means all of the following: emails, text messages (SMS), voice messages, sound messages, image message, multimedia messages. You must include an opt-out mechanism in every electronic marketing message that is sent.

Withdrawing consent

- If an individual withdraws their consent to be marketed, you must stop. Many data subject rights under the GDPR are not absolute eg there are some restrictions on access, but withdrawal of consent to direct marketing is an absolute right;
- You should be able to update your records on receipt of any changes. If an individual objects to marketing under the GDPR you must ensure that you have processes in place to action his/her request as quickly as possible, and within the one-month timeframe. You may confirm to the individual that they have been removed from the marketing contacts list; this is not considered further direct marketing. You are also to inform the DPO if you receive a request to stop processing for direct marketing purposes;
- You may maintain a 'suppression list' of individuals who don't want to receive marketing ie individuals who have opted-out. You should keep this list up to date and accurate, and consider which employees require access to it;
- If employees in other areas of Carlow College carry out marketing and promotional activities on behalf of Carlow College, there is a danger that they may market individuals who have opted-out of receiving marketing from the College. Aside from distributing a 'suppression list' to those employees, the other option is to have a clear rule, communicated to employees, that all marketing and promotion is to be done by the Marketing Office only;
- It must be as easy to withdraw consent as it was to give it. The means the process of withdrawing consent should be an easily accessible one-step process using the same process used to give permission eg 'Email us at marketing@carlowcollege.ie or phone us at 059-9153200 if you wish to withdraw your consent' is acceptable. 'Phone us on Mondays if you wish to withdraw consent' is not acceptable; neither is having data subjects go through several pages of a website to unsubscribe;
- Withdrawal of consent does not affect the lawfulness of processing before the consent was withdrawn.

Involvement of external companies

You should not use bought-in lists for emails, texts or automated calls unless you have proof of opt-in consent within the last six months, which specifically names Carlow College;
If any external companies are processing personal data, you need to have a contract in place (eg website developer).

Data quality

- Where an individual advises that their data is inaccurate and wishes to exercise his/her right to rectification, the Marketing Office is to update contact details as soon as possible, and within one month. You are to inform the DPO of such a request;
- If accuracy of data provided by individuals is an issue, consider inserting a 'confirmation' field on web forms, wherever possible eg field for email address and then an email confirmation field, which only submits if they match.

Electronic marketing

- Electronic mail means all of the following: emails, text messages (SMS), voice messages, sound messages, image message, multimedia messages;
- You must include an opt-out mechanism in every electronic marketing message that you send;
- When sending direct marketing email messages to a group, ensure that is sent using the 'bcc' mechanism.

Privacy-friendly data collection

Where you collect contact details for marketing purposes at Open Days or other events the most privacy-friendly mechanism should be used. Bound volumes in which individuals can see each other's personal data are not recommended. It would be better to either use a discrete sheet of paper that each person completes and hands back, or to collect the data via a device such as an iPad on which each person completes a discrete form. Ensure that the format used is a consent form, following the template given at Appendix 1.

Drones

If you are using drones to record footage for any purpose, there are specific Data Protection guidelines in place: https://www.dataprotection.ie/docs/Guidance-on-the-use-of-Drone-Aircraft/1510.htm;
The Marketing Office is to ensure compliance with this Guidance.

Project design

- There are tools called Data Protection Impact Assessments (DPIAs), which are useful when planning projects that involve processing personal data. DPIAs involve looking at project proposals, privacy risks and implementing mitigating measures. They can be scaled to size. Further information about DPIAs is available in the Data Protection Policy;
- The data which you collect must be adequate, relevant and not excessive. Information must not be collected unless it is actually intended to use it. For each marketing project that involves collecting personal data, plan out what information you require. You must not collect data just because it *might* be useful.

Use of personal data in marketing materials

- Where the Marketing Office uses personal data in its promotional materials, the consent of identified and identifiable persons must be obtained. It is recommended that consent is in a written format;
- Remember that when you use consent as the basis for processing data, an individual may withdraw their consent. They may also submit a request for erasure of their data. Right of erasure is a data subject right under the GDPR. If you receive a request for erasure of personal data send it to the DPO for processing;
- Again, if seeking a release to use an individual's personal data, consider how long it is reasonable that a release endures.

Right of erasure of personal data

- The right of erasure of personal data, also known as 'the right to be forgotten', applies in six scenarios:
    - Where the personal data is no longer necessary in relation to the purposes for which it was collected;
    - When the data subject withdraws his/her consent and there is no other legal ground for the processing;
    - When the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
    - The personal data have been unlawfully processed;
    - The personal data have to be erased to comply with a European Union or Member State legal obligation; or
- The personal data have been collected in relation to the offer of information society services to a child.
- Where a controller (the College) complies to the request, the controller must take reasonable steps to inform other controllers to whom the data has been disclosed, of the request to erase any links to, copies or replications of, the personal data in question. This is challenging for controllers who process personal data in an online environment, for example, on social networks or websites. The controller must also inform the data subject about those recipients, if so requested;
- Given this information, where the Marketing Office uses or supplies personal data in marketing materials, a record should be kept of when and where data was used;
- There are grounds for a controller to refuse to comply with a request for erasure:
    - To exercise the right of freedom of expression and information;
    - To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
    - For public health purposes in the public interest;
    - Archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
    - The exercise or defence of legal claims.
- When you use personal data in marketing materials eg in published graduate profiles, consider how much personal data you need to use to communicate your message. Remember the rule to process data in a way that it is adequate, relevant and not excessive. You might consider, for example, whether a person needs to be named at all; whether a first name is sufficient where you do want to personalise it; whether you need to give a person's age. Such questions should be considered on a case by case basis.

Special categories of personal data

- The following categories of data are 'special categories of personal data' under the GDPR:
    - 'data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.
- Data concerning criminal convictions was 'sensitive personal data' under the Data Protection Acts 1988 and 2003. It is not a special category data under the GDPR but continues to benefit from special protection;
- If you are using such data in marketing materials you should obtain 'explicit consent.' Another possible basis is that the data has manifestly been made public by the data subject. The legal bases for processing special categories of personal data are given in Article 9 of the GDPR;
- The GDPR encompasses the concepts of both 'consent 'and 'explicit consent', which is not defined in the legislation;
- 'Explicit consent' is an area where further guidance may be available in the future. For now, 'explicit consent' should be in writing. The data subject should be informed in writing where the data will be held, who will use it, who it will or may be shared with, how long it will be retained, and it should be specified exactly what information is involved (eg 'health data' or 'religion' etc). Data subject must understand possible risks to their rights and freedoms;
- Most of the special categories of personal data will likely not apply to the Marketing Office. One scenario which may arise in third level institutions is 'success stories' using information regarding learners with learning differences or disabilities. Such information constitutes health data, which is special category data. Firstly, it is recommended that the Marketing Office does not use special categories of data in its marketing materials or, at minimum, very carefully considers its use if it proposed to do so, and the risks to the rights and freedoms of the data subjects. This is an area where a DPIA would be useful;
- The GDPR considers that the processing of photographs is not automatically considered as falling within special category personal data (for example, if a person's race may be determined from the photograph). Photographs are only considered as such if they allow the unique identification or authentication of an individual as a biometric (for example, in an electronic passport).

<u>Taking photographs at events</u>

- Where children are attending events in Carlow College and are in the care of parents, teachers or other responsible persons eg group leader of some type and you wish to take photographs, ask the responsible person if there is consent to photograph the children and what the consent covers eg publication on social media. The College's Social Media Policy may also be applicable here. Check in case some children are not consented for photography. Gaining consent in terms of children is problematic. There is the question of whose consent is needed in a specific situation and it may be some combination of child, parent and responsible persons;
- It is recommended that the Marketing Office introduce procedures around the taking and use of photographs of College events, such as conferring ceremonies: firstly, to inform those attending that photographs will be taken, who will have access to them and how they will be used; and secondly, to seek consent, where appropriate. Consent may be either verbal or written, depending on how it is intended to use the photographs;

- Where employees of Carlow College, other than Marketing Office employees, take photographs at College events, this is an area that merits discussion and procedure.

Photographers

Always check with commercial photographers about copyright and that they understand and agree with how you intend to use images. Unless they sign over copyright, they own it.

Conducting surveys

- It is recommended that the Marketing Office coordinates surveys of learners on behalf of Carlow College. It is suggested that an organised calendar of surveys is set out; that surveys are on topics approved by the Office of the Registrar; and that questions are carefully formulated. If this recommendation is implemented, Marketing Office employees might assist others to design their surveys;
- Only seek as much personal data as you require. Unless you require to be able to identify persons who are surveyed, surveys should be anonymous;
- Remember also that if you are surveying small groups individuals, they can sometimes be identified indirectly by putting different pieces of information together. Review your survey results before release to ensure that this does not happen, especially if the survey was publicised as 'anonymous';
- It should also be decided who will hold the raw data (ie whether the office requesting the survey will get it or just anonymised results of the survey). What is decided must be transparent, justifiable and fair. Unless the raw data is *required* by the other employee, it should not be shared. Persons who are surveyed should be told who will have access to the data at the time the data is collected;
- Where you conduct a survey and collect personal data as part of it, delete the raw data as soon as it is no longer required or pseudonymise it or anonymise it. Pseudonymised data is still personal data. Anonymised information is not personal data as the data subject cannot be identified;
- Be conscious of what data you are collecting. If you are designing a survey around special categories of personal data, extra care must be taken. For instance, consider what safeguards might be implemented if the Counselling Service asked for assistance in surveying their clients. A survey such as this should be anonymous. It may be more appropriate for the responses to the survey to be sent directly to the Counselling Service rather than the Marketing Office;
- If you want to use personal data collected in surveys for a purpose other than the survey eg marketing, you must seek consent for this at the time that the data is collected. This may be inappropriate in some instances, for example, to ask Counselling Service clients for contact details for direct marketing would not be acceptable.

Current learner personal data

Where you acquire current learner data from other offices and departments of Carlow College for recruitment of new learners you must ask for anonymised information only. Anonymised data is not personal data. It is acceptable to receive information on the number of learners, the names of schools, county and gender but there would seem to be no justification for personal data to be released to the Marketing and School Liaison Office for the purpose of recruitment. In this context, personal data would mean typically name, address, ID number, PPSN or anything else by which a learner is identifiable. You must not link information received for another purpose to identify an individual.

Purpose limitation

This is a GDPR principle by which personal data collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The Marketing Office may collect and process data for a variety of purposes, sometimes on its own behalf, sometimes on behalf of other departments and office within Carlow College. In addition, data acquired from different sources for different purposes must not be used to build 'profiles' of data subjects.

Appendix 1
Sample consent form

Carlow College, St. Patrick's
Keep in touch with us! Our events and services might interest you. We are a third level college and provide courses in the areas of Humanities, Social Care and Community and Citizenship. We organise public lectures and conferences on related topics.

Please fill in the contact details you want us to use to keep in touch with you:
Name
Address
Email
Telephone number

Please tick the boxes to tell us what you would like to receive information on:
□ Humanities courses
□ Social Care courses
□ Community & Citizenship courses
□ Public lectures and conferences

Please tick the boxes below to tell us all the ways you are happy to hear form us:
□ Yes, I would like to receive communications by email
□ Yes, I would like to receive communications by telephone
□ Yes, I would like to receive communications by text message
□ Yes, I would like to receive communications by post

By signing this form, you are consenting to Carlow College, St Patrick's contacting you.
Signature
Date
You can find out more about how we use your data in our Privacy Notices, which are available on our website. You can grant consent to none, some or all the purposes. You can withdraw or change your consent at any time by contacting the Marketing Office at Carlow College, St. Patrick's, College Street, Carlow; or marketing@carlowcollege.ie; or 059-9153200. We will stop processing your personal data for this purpose once you have withdrawn consent, but this will not affect of lawfulness of the processing prior to withdrawal of consent. We do not share your data with any third party.

7. Carlow College, St. Patrick's: Personal Data Breach Response Plan

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Internal notification

Any employee who becomes aware of an actual or suspected personal data breach or that data has been placed at risk is to notify the DPO without delay. This includes a notification received by an employee from any processor or joint controller of Carlow College of any such incident.

The communication to the DPO is to be made by telephone or in person. Email is not acceptable as reported incidents must be responded to promptly. The employee must ensure that the DPO receives the information.

If the employee does not succeed in contacting the DPO, he/she is to contact the Office of the President, the Director of Operations or his/her line manager, in that order, without delay. Communication is to be by the same means as described in point 2.

Assessment of situation

An assessment into the circumstances of the reported breach will commence as soon as possible. The scale of an assessment will be influenced by the extent suggested by the situation.

Normally, the assessment team will include the President, the Director of Operations and the DPO.

Other employees may join the assessment team depending on the circumstances. For example:

- A representative of the Office of the Registrar may participate if the situation pertains to learner data;
- The Human Resources Office may participate if employee data is involved;
- The IT Officer may join the investigating team if electronic data is implicated;
- The Finance Officer may be involved if financial data is involved.

The DPO will advise the assessment team.

The assessment team will determine:

- Whether a breach has occurred;
- The nature of the personal data involved (including whether it includes special categories of personal data);
- The cause of the breach;
- Establish whether there is anything that can be done to recover a loss or contain further loss. This may involve engaging the services of contractors/processors;
- The number of individuals who are affected;
- The potential risk to affected individuals.

The results of the aforementioned assessment will determine what notifications and further actions are required, if any. Complex, large-scale breaches will require thorough investigation.

An Garda Síochána will be notified in cases involving criminal activity.

Notifying a personal data breach to the Office of the Data Protection Commissioner (DPC)

Controllers have a mandatory obligation to report data breaches to their supervisory authority (the DPC in Ireland) within 72 hours of becoming 'aware' of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. An example of an incident that does not require reporting might be where personal data is already publicly available.

When a controller notifies a breach to the DPC, it should, at the minimum:

- Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- Communicate the name and contact details of the DPO or other contact point where more information can be obtained;
- Describe the likely consequences of the personal data breach;
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The controller should also inform the DPC if it intends to provide more information at a later point. The DPC may request further details of part of its investigation into a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach. The DPC is empowered to require controllers to inform data subjects about the breach.

If notification is not made within 72 hours, a reasoned justification for the delay must be provided. The 72 hours does not take weekends, public holidays etc into account. 'Awareness' begins when the controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

Notifying personal data breaches to data subjects

Controllers have to notify data subjects where the data breach is likely to result in a 'high risk' to affected data subjects. WP29 (now the European Data Protection Board; hereafter EDPB) advice is that 'high risk' exists when the breach may lead to physical, material or non-material damage for the individuals whose data has been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that involves racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offended or related security measures, the breach should be considered high risk.

Notification to data subjects is not required where:

- The controller has implemented appropriate technical and organisational measures that render the personal data unintelligible to anyone not authorised to access it, such as encryption; or

- The controller has taken subsequent measures which ensure that the high risk to data subjects is not likely to materialise; or
- It would involve disproportionate effort, in which case there should be a public communication instead.

In the event that Carlow College informs data subjects of a data breach, the most appropriate method will depend on the circumstances. In general, data subjects must be contacted by some personally directed method rather than a general public notice.

Notification may be by telephone call, SMS, email or letter. Public notices may also be posted on the College website or social media accounts.

When notifying data subjects of a breach, the controller should provide the following information, at least:

- A description of the nature of the breach;
- The name and contact details of the DPO or other contact point;
- A description of the likely consequences of the breach; and
- A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where appropriate, specific advice should be given to data subjects to protect themselves from possible adverse consequences of the breach, such as resetting passwords where access credentials have been compromised.

At the request of the President, The Marketing Office may assist in communicating with data subjects and responding to any media queries.

Required actions when Carlow College is a processor

Carlow College is a processor in terms of some its data processing. Processors have to notify controllers of breach situations. WP29 (now the EDPB) guidance is that processors notify controllers immediately, with further information about the breach provided in phases as information becomes available. Notifications to controllers will be in writing.

The DPO will act as a point of contract for controllers at the request of Carlow College. Data sharing agreements may impose a timeframe for notification to controllers.

Review of response to breach

In the aftermath of a personal data security breach, a review of the incident may take place to ensure both that the steps taken during the incident were appropriate and effective, and to identify any organisational or technical measures that require updating to minimise future risk of a similar incident.

Register of breaches

Controllers must keep an internal record of all data breaches, a description of the facts of the breach, its effects and the remedial action taken.

It is WP29 (now EDPB) advice that the register of breaches should also include its reasoning for decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers that the breach is unlikely to result in a risk to the rights and freedoms of individuals. The DPO will keep this record on behalf of Carlow College.

8. Rules for Employees: Safeguards to Protect Personal Data

Carlow College is obliged to implement measures known in the GDPR as 'technical and organisational and measures' to safeguard personal data.

Employees are to familiarise themselves with the following safeguards.

The preeminent safeguard is:
If you are not sure how to proceed in a matter involving personal data, delay action and seek advice.

This is not in any way intended to be an exhaustive list of safeguards. Queries regarding IT security measures should be addressed to IT Services.

When collecting and creating personal data:

- Don't collect personal data unless you require it
- Double check that you are sending an email to your intended recipient
- Official College records should be saved and kept in the College IT or manual systems
- Don't use personal devices or accounts to create records
- Simple updates may be made eg change of address on a system, but otherwise, don't alter a document created by another employee
- Employees are not to access records that they are unauthorised to view, that is, any record which is unrelated to their functions or for which they have not been granted access permissions
- Photographs of identified and identifiable persons are personal data. Ask permission before taking photographs and only use them in ways for which you obtain consent
- Ensure that your communications are written in an objective, truthful, responsible and accurate manner
- If you work remotely you must take appropriate measures to ensure the confidentiality and security of personal data and other records
- Pseudonymise or anonymise personal data when it is no longer necessary to identify individuals
- Carry out Data Protection Impact Assessments, where required
- Consider Data Protection issues at an early stage if you are designing a new project or processing activity
- Review your policies and procedures for data handling on a regular basis
- Carry out audits on data quality eg check for errors
- Design forms to collect the minimum amount of personal data necessary to fulfil a purpose
- Collect personal data in a privacy friendly manner. Sign-in books used by multiple persons for recording their contact details might be replaced with individual use forms in paper or electronic formats
- When purchasing software ensure that it permits audit logs
- Personal data is not to be posted on public noticeboards
- Ensure that personal data is kept up to date and make requested changes promptly

- Check back with data subjects that what you have recorded is accurate

When disclosing personal data:

- Explain to parents/guardians and family members that the College only releases personal data of learners with their consent, except in extremely limited circumstances, such as a medical emergency
- Student ID numbers are personal data as they are linkable to an individual. They cannot be used to pseudonymise information about learners
- Double check your recipient when sending an email
- Send group emails via bcc where it's not appropriate that recipients can see each other's email address, for example, direct marketing emails, or where membership of a group of individuals should not be disclosed to the others eg cancellation of a Counsellor's appointments; or to a number of witnesses in a disciplinary case
- Password-protect attachments containing personal or confidential data
- Circulate personal data and business records both to colleagues and externally on a need to know basis only. Data sharing should accord with the Privacy Notices
- If authorised employees from other departments require to borrow files from your office, implement a sign out/in book. Agree a borrowing period and issue a reminder if they are not returned
- Don't share personal data (or other confidential information) acquired through your official duties on social media

When disposing of personal data:

- Dispose of personal data and other business and confidential records in a secure manner. Shred them. Every employee is responsible for the secure disposal of records in their custody. Records are not to be disposed of in wastepaper or recycling bins
- Dispose of personal data and other records in accordance with the Records Retention Schedules and Records Destruction Procedure if their use is expired
- Some personal data and other records have been designated 'archival' which means that they are kept on an ongoing basis. Keep these records safe and secure; transfer them to the Delany Archive
- Ensure that you return to IT Services computers and other devices on which personal data and confidential records are stored
- Ensure that if you keep College-owned records, including personal data, on a personal device that you dispose of items in a secure manner

Keeping data secure:

- All personal data and other official records of Carlow College are confidential. It is the duty of all employees to maintain and protect this confidentiality

- Notify the DPO of any incident where data has been placed at risk or you suspect a potential or actual breach
- If the security of a personal device which contains personal data or business records of Carlow College has been compromised in any way, employees must notify the DPO and their line manager
- Lock your computer screen when you leave your office
- Lock your office if it is unattended
- Don't leave your key in your office door
- Don't leave unauthorised persons alone with personal data
- Don't allow your computer screen to be viewable from a public area or to an unauthorised person
- Keep paper records in locked storage units
- Return paper files to their storage units promptly
- Don't remove personal data or other confidential records from the College premises unless necessary
- Don't leave personal data or other confidential records on view in your car or in your car overnight
- Assignments and examination scripts are not to be corrected in a public place
- Personal data or other confidential records are not to left in publicly accessible areas, either in the College buildings or other premises
- Don't store personal data on removable devices such as memory sticks unless necessary
- Password-protect documents stored on removable devices
- Don't print unnecessary paper copies of documents containing personal data
- Keep your passwords private to you. You are not to share them with any other person
- Change your passwords regularly
- Don't make passwords easy to guess. Passwords should contain a mixture of letters and other characters
- Don't use the same password for multiple accounts
- Transfer personal data and other records to the Archive for safekeeping if you no longer require them and they are identified in the Records Retention Schedules as archival
- Don't leave personal data or other confidential records unattended at photocopiers
- Don't save personal data or other confidential records to shared laptops or other devices
- Consider if remote wipe technology would be proportionate when buying devices

New colleagues:

- Appoint a 'buddy' to new employees to explain procedures for handling personal data and other records
- Work experience volunteers should have limited or no access to personal data and other confidential records